ABSTRACT

The bread pudding protocol of the present invention represents a novel use of proofs of work and is based upon the same principle as the dish from which it takes its name, namely, that of reuse to minimize waste. Whereas the traditional bread pudding recipe recycles stale bread, our bread pudding protocol recycles the "stale" computations in a POW to perform a separate and useful task, while also maintaining privacy in the task. In one advantageous embodiment of our bread pudding protocol, we consider the computationally intensive operation of minting coins in the MicroMint scheme of Rivest and Shamir and demonstrate how the minting operation can be partitioned into a collection of POWs, which are then used to shift the burden of the minting operation onto a large group of untrusted computational devices. Thus, in accordance with one illustrative embodiment of the present invention, the computational effort invested in the POWs are recycled to accomplish the minting operation.